

13/589906

JAP6 Rec'd PCT/PTO 18 AUG 2006

Docket No.: 2004P0147

C E R T I F I C A T I O N

I, the below named translator, hereby declare that: my name and post office address are as stated below; that I am knowledgeable in the English and German languages, and that I believe that the attached text is a true and complete translation of PCT/EP2005/050190, and amended pages, filed with the European Patent Office on January 18, 2005.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Hollywood, Florida


Rebekka Pierre

August 18, 2006

Lerner Greenberg Stemer LLP
P.O. Box 2480
Hollywood, FL 33022-2480
Tel.: (954) 925-1100
Fax.: (954) 925-1101

1 Description

2
3 Method for the control and evaluation of message traffic of a
4 communication unit by means of a first network unit within a
5 mobile radio system, pertaining communication unit and first
6 network unit

7
8 The object of the invention is to provide the control and
9 evaluation of the message traffic of a communication unit by
10 means of a first network unit within a mobile radio system in a
11 simple and efficient manner. This object is achieved by the
12 following method in accordance with the invention.

13
14 Method for the control and evaluation of message traffic of a
15 communication unit by means of a first network unit within a
16 mobile radio system, in that all the messages of the message
17 traffic are forwarded via the first network unit, in that by
18 means of the first network unit a decision is made with the aid
19 of one or more items of useful information from the
20 communication network KE as to whether one or more messages are
21 to be forwarded to a second network unit for further processing
22 or are to be blocked, and in that a decision is made by means
23 of the first network unit with the aid of one or more items of
24 useful information from the communication unit as to whether
25 the particular message of the message traffic is to be logged
26 by the first network unit in a logfile.

27
28 By means of the method in accordance with the invention, the
29 message traffic of a communication unit is controlled and
30 evaluated in an advantageous manner. Using one or more items of
31 useful information of the particular communication unit,
32 different and individual decision rules for control and
33 evaluation can be used for various communication units.

1
2 Furthermore, by means of the method in accordance with the
3 invention the logging of the message traffic of an application
4 of the particular communication unit is enabled in an
5 advantageous manner. Because the logging takes place at
6 application level, the logging can be made dependent on the
7 content of the individual messages, i.e. on the message data.
8 Thus, the data quantity of messages with multimedia content,
9 such as video sequences or voice recordings, can be registered
10 during the logging as a chargeable data volume, and messages
11 with control information can be excluded from the logging.

12
13 The invention also relates to a first network unit for control
14 and evaluation of message traffic of a communication unit
15 within a mobile radio system, with a receiving unit by means of
16 which all the messages of the message traffic of the
17 communication unit can be received, with a transmitting unit by
18 means of which all the messages of the message traffic can be
19 transmitted, and with a processing unit by means of which it
20 can be decided, on the basis of one or more items of useful
21 information from the communication unit, whether at least one
22 message of the message traffic is to be forwarded to a second
23 network unit for further processing or is to be blocked, and by
24 means of which it can be decided, on the basis of one or more
25 items of useful information from the communication unit whether
26 at least one message of the message traffic is to be logged in
27 a logfile by the first network unit.

28
29 The invention also relates to a communication unit where the
30 message traffic within a mobile radio system is controlled and
31 evaluated by a first network unit, with a receiving unit by
32 means of which all the messages of the message traffic can be

1 received, and with a transmission unit by means of which all
2 the messages of the message traffic can be transmitted.

3

4 Other developments of the invention are given in the subclaims.

5

6 The invention and its developments are explained in more detail
7 in the following, with reference to drawings.

8

9 The drawings are as follows:

10

11 Figure 1 A schematic drawing showing an arrangement for
12 controlling and evaluating message traffic of a
13 communication unit by means of a network unit that
14 consists of a group of network elements within a
15 mobile radio system, in accordance with a first
16 variant of the method in accordance with the
17 invention, including associated modifications,

18

19 Figure 2 A flow diagram of possible message traffic for an
20 example of an application in accordance
21 with Figure 1,

22

23 Figure 3 A schematic representation of a possible construction
24 of an item of called-up useful information with two
25 user identities,

26

27 Figure 4 A schematic representation showing an arrangement for
28 controlling and evaluating message traffic of a
29 communication unit by means of a network unit,
30 consisting of a group of network elements within a
31 mobile radio system, using the IMS standard in
32 accordance with another variant of the method in

1 accordance with the invention, including associated
2 modifications.

3
4 Figure 5 A flow diagram of possible message traffic for an
5 example of an application in accordance with Figure
6 4.

7
8 Figure 6 A possible expansion of the flow diagram for an
9 exemplary embodiment in accordance with Figure 5.

10
11 Figure 7 A possible flow diagram of message traffic for a
12 further example of an application with messages with
13 SIP signaling and messages with useful data between a
14 communication unit and network unit being associated.

15
16 1. First exemplary embodiment

17 1.1. Device

18 Figure 1 shows a first possible device for implementation of
19 the method in accordance with the invention. Figure 1 shows a
20 simplified representation of a possible network architecture.
21 In the center of Figure 1 is a home network HN (HN - Home
22 Network) of a communication unit KE, that in Figure 1 stays in
23 a visited network VN (VN - Visited Network). This case is also
24 generally known as "roaming". The home network HN and the
25 visited network VN are located in a mobile radio system MS. The
26 communication unit KE is, for example, mounted in a radio unit
27 to the GSM standard (GSM - Global System for Mobile) or UMTS
28 standard (UTMS - Universal Mobile Telecommunication System).
29 This communication unit KE enables messages to be transmitted
30 by means of a transmitting unit SE1 and also messages to be
31 received by means of its receiving unit EE1. Furthermore, the
32 communication device KE has a processing unit VE1, that permits
33 the implementation, e.g. of an application AP. This application

1 AP is especially a browser application or a push-to-talk
2 application. The receiving unit EE1, the transmitting unit SE1
3 and the processing unit VE1 are connected by means of a
4 connecting network XN1 and therefore able to exchange
5 information.

6

7 The communication unit KE is connected in the visited network
8 VN with a first network element NW1 through a first connection
9 V1. This first network element NW1 is especially a GGSN (GGSN -
10 Gateway GPRS Support Node) (GPRS - General Packet Radio System).
11 This first connection V1 is established with the aid of the
12 procedure called the PDP Context Activation Procedure (PDP -
13 Packed Data Protocol), as described in 3GPP - 3rd Generation
14 Partnership Project) TS 23.060 Version 5.3.0 "General Packet
15 Radio Service GPRS", Stage 2. During the establishment of this
16 first connection V1, it is specified that this first connection
17 V1 may be used only for the exchange of messages, for example
18 messages with useful data ND, between the communication unit KE
19 and the first network element NW1. Useful data ND is preferably
20 understood to be data such as an image or a voice recording,
21 but not signaling information. All messages with useful data ND
22 transmitted on this first connection V1 are automatically
23 forwarded from the first network element NW1 via a second
24 connection V2 to a second network element NW2. The second
25 network element NW2 is preferably a data gateway.

26

27 The second network element NW2 on the one hand has a fourth
28 connection V4 in a public, packet-oriented network PN (PN -
29 Public Network), such as the Internet. The public, packet-
30 oriented network PN includes, for example, a second network
31 unit NE2, such as a server with video sequences. On the other
32 hand, there also exists a third connection V3 to a third
33 network element NW3 that is located in the home network HN of

1 the communication unit KE. The third network element NW3 is
2 preferably a data gateway.

3

4 Furthermore, the third network element NW3 is networked with a
5 database HSS, preferably a home subscriber service, through a
6 fifth connection V5. This database HSS contains user-related
7 information of the communication unit KE. Furthermore, the
8 third network element NW3 is connected via a sixth connection
9 V6 with the public packet-oriented network PN. In addition, the
10 second network element NW2 in the visited network VN can be
11 directly connected to the database HSS. This is shown in Figure
12 1 by a dotted seventh connection V7.

13

14 A first network unit NE1 can consist of several network
15 elements NEE. In Figure 1 the first network element NE1
16 includes the first, second and third network elements NW1, NW2,
17 NW3. In a case where the communication network KE is located in
18 its home network HN, the second and third network element NW2
19 or NW3 can be located in a single network element that provides
20 the functionalities of the second and third network elements
NW2 or NW3. The first network element NE1 includes a
22 transmitting unit SE2 for forwarding messages and a receiving
23 unit EE2 for receiving messages. In addition, it contains a
24 processing unit VE2 for controlling and evaluating data traffic
25 of the application AP of the communication unit KE. The
26 transmitting unit SE2, the receiving unit EE2 and the
27 processing unit VE2 can exchange information through a
28 connecting network XN2. In Figure 1, each network element NEE
29 contains its own transmitting unit, its own receiving unit, its
30 own processing unit and its own connecting network. The example
31 in Figure 1 shows the transmitting unit SE2, the receiving unit
32 EE2, the processing unit VE2 and the connecting network XN2 for
33 the second network element NW2.

1

2 1.2 Request message

3 In the following, the authentication of a communication unit is
4 explained in more detail with the aid of Figure 1. This
5 authentication is necessary so that the second network element
6 NW2 can determine whether a communication unit is actually that
7 which it claims to be or whether this communication unit is
8 authorized to exchange messages with the public packet-oriented
9 network PN via the second network element NW2.

10

11 Figure 2 shows a flow diagram of possible message traffic which
12 is necessary for the authentication. In particular, this deals
13 with the problem of message exchange between the communication
14 unit KE and the public packet-oriented network PN.

15

16 If the communication unit KE requests messages, for example
17 messages with useful data ND, from the public packed-oriented
18 network PN or wishes to transmit messages to same, the
19 communication unit KE sends a request message AN to the second
20 network element NW2. In a case where the HTTP (Hyper Text
21 Transfer Protocol) is used, this request message AN is an HTTP
22 request. This request message AN contains a destination address
23 EA from which useful data ND is requested and/or sent. The
24 destination address EA can be in the form of a URI (Unique
25 Resource Identifier). To authenticate the communication unit
26 KE, a mechanism in accordance with the IETF (International
27 Engineering Task Force) RFC (Request For Comments) 3310 "Hyper
28 Text Transfer Protocol (HTTP) Digest Authentication Using
29 Authentication and Key Agreement (AKA)", see www.ietf.org,
30 can be used. For this purpose, an information line with the
31 name "Authorization" is inserted into the request message AN.
32 This mainly contains information regarding a user identity NID.

33

1 1.3 User identity

2 A user identity NID provides a unique identification of a
3 specific communication unit, e.g. the communication unit KE. By
4 means of the information line with this user identity NID, the
5 second network element NW2 can determine, in a first decision
6 step A1, the network, e.g. the home network HN, to which the
7 communication unit KE belongs. It is also determined whether
8 the second network element NW2 has already stored one or more
9 items of authentication information for the requesting
10 communication unit KE. Because the second network element NW2
11 still has no authentication information of this kind, the
12 second network element NW2 forwards the request message AN to
13 the third network element NW3. It is assumed that the third
14 connection V3 is protected and no third party is able to
15 intercept, change or read messages.

16

17 1.4 Useful information

18 In the following step, the third network element NW3 uses a
19 third message N3 containing the user identity NID to request,
20 from the database HSS, preferably the following useful
21 information NI for the communication unit KE.

- 22 - One or more second keys SP2 that are to be used for
23 authentication and encoding of messages for the
24 communication unit KE of the second network element NW2.
25 - A challenge HEF that is to be used for authentication by
26 the communication unit KE, e.g. refer to IETF RFC 3310.
27 - One or more filter instructions FW.

28 In the following it is assumed that only a second key SP2 is
29 requested from the database DB.

30

31 1.5 Filter instruction

32 These filter instructions FW particularly include one or more
33 of the following criteria:

- 1 - One or more positive destination addresses PEA, that can
2 be addressed by the communication unit KE.
- 3 - One or more negative destination addresses NEA, that
4 cannot be addressed by the communication unit KE
- 5 - One or more destination addresses XEA that are to be
6 logged by the first network unit NE1. Logging by the
7 second network element NW2 is shown in Figure 1.

8

9 With the aid of these filter instructions FW, the second
10 network element NW2 is enabled to limit access by the
11 communication unit KE to one or more specific destination
12 addresses EA in the public packet-oriented network PN. In
13 addition, these filter instructions FW can also be used to
14 inform the second network element NW2 to record accesses to
15 certain destination address EA separately from other accesses.
16 Because several user identities NID can be allocated to one
17 communication unit KE, one or more filter instructions FW can
18 be explicitly allocated to a specific user identity NID. It is
19 thus appropriate if one user identity NID is allocated in each
20 case to an application AP.

21

22 With the aid of a fourth message N4, this useful information NI
23 is transmitted from the database HSS to the third network
24 element NW3. The third network element NW3 subsequently
25 transmits this useful information NI in a fifth message N5 to
26 the second network element NW2. In a case where the HTTP
27 protocol is used for this purpose, the useful information NI
28 specified for the challenge HEF of the communication unit KE is
29 inserted in an information line with the name "WWW-
30 Authenticate", see IETF RFC 3310 and IETF RFC 2617 "HTTP
31 Authentication: Basic and Digest Access Authentication".
32 All second keys required for encoding, authentication and
33 protection of integrity are dealt with in a similar manner. In

1 addition, an expected answer AEH to the challenge HEF can be
2 contained in this fifth message N5. This enables the second
3 network element NW2 to check the response AGH sent by the
4 communication unit KE in response to the challenge HEF against
5 the expected answer AEH for correctness. In this case, it is
6 not necessary to forward this response AGH to the third network
7 element NW3 to check the authenticity.

8

9 One or more filter instructions FW can be contained in a new
10 type of message body in this fifth message N5, that for example
11 is formed as an HTTP message using the HTTP protocol. This new
12 type of message body can be identified by means of a unique
13 description. This is appropriate in practice because this
14 unique description is contained in the actual HTTP message in
15 an information line with the name "Content-Type", that, for
16 example, is formed according to the IETF RFC 2045 standard
17 "Multipurpose Internet Mail Extensions (MIME) Part One: Format
18 of Internet Message Bodies". This enables the second network
19 element NW2 to determine the content of the HTTP message just
20 by using this unique description, for example to determine
21 whether it contains filter instructions FW.

22

23 Figure 3 is an example of the structure of several filter
24 instructions FW contained in a message body NK. This message
25 body NK has two lists L11, L12 or L21, L22 for each user
26 identity NID1 or NID2 respectively. The first list L11 or L21
27 of the user identity NID1 or NID2 contains a list of the
28 destination addresses XEA to be logged. The second list L12 or
29 L22 of the relevant user identity NID1 or NID2 provides one or
30 more negative destination addresses or NEA that cannot be
31 addressed by the communication unit KE and/or one or more
32 positive destination addresses PEA that can be addressed by the
33 communication unit KE.

1
2 After receipt of the fifth message N5, the second network
3 element NW2, in a second step A2, takes the second key SP2 from
4 the information line with the name "WWW-Authenticate". Using
5 the information line with the name "Content-Type", the second
6 network element NW2 detects that one or more filter
7 instructions FW are contained in the message body NK, and also
8 takes these. The second network element NW2 then forwards this
9 modified fifth message N5, as a sixth message N6, to the
10 communication unit KE. Following this, the communication unit
11 KE takes the challenge HEF from the information line with the
12 name "WWW-Authenticate". With the aid of one or more of the
13 items of information stored on a SIM (Subscriber Identification
14 Model) card of the communication unit KE, a suitable first key
15 SP1 is now calculated that can be used for the encoding of the
16 messages between the communication unit KE and the second
17 network element NW2, and also for authentication and protection
18 of the integrity. The first key SP1 and the associated second
19 key SP2 form a correlated key pair SCP. Furthermore, the
20 communication unit KE calculates the response AGH to the
21 challenge HEF by using the first key SP1.

22

23 1.6 Modified request message

24 In a next step, the communication unit KE sends a modified
25 request message ANM to the second network element NW2. In a
26 case where the HTTP syntax is used for the modified request
27 message ANM, this modified request message ANM corresponds to
28 an HTTP request. This modified request message ANM contains
29 both the destination address EA from which the communication
30 unit KE is to send useful data ND and also an information line
31 with the name "Authorization". This information line also
32 contains, in addition to the user identity NID, the response
33 AGH to the challenge HEF.

1
2 After receipt of the modified request message ANM, the second
3 network element NW2, in a third decision step A3, uses the user
4 identity NID contained in the information line with the name
5 "Authorization" to check whether the second network element NW2
6 has already stored authentication information for this
7 communication unit KE. This is now given after the previous
8 step of this exemplary embodiment has been completed.
9 Accordingly, the second network element NW2 takes the
10 information line with the name "Authorization" from the
11 modified request message ANM. With the aid of the second key
12 SP2 stored in the second network element NW2, the response AGH
13 to the challenge HEF is checked for correctness in a next step.
14 If the transmitted response AGH is not correct, the modified
15 request message ANM is rejected by means of a tenth message
16 N10. If the check shows correct agreement with the expected
17 response AEH to the challenge HEF, then, in a fourth decision
18 step A4, a check is carried out to determine whether the
19 destination address EA contained in the modified request
20 message ANM can be addressed by the communication unit KE. In a
21 case where this destination address EA matches a negative
22 destination address NEA, the modified request message ANM for
23 transmission of useful data ND is rejected. This is notified to
24 the communication unit KE by means of a tenth message N10.
25 Alternatively, instead of the check of the destination address
26 EA with the aid of at least one negative destination address
27 NEA, the check can be carried out using at least one positive
28 destination address PEA. In this case, a check is carried out
29 to determine whether the destination address EA corresponds to
30 a positive destination address PEA. If it does not, the
31 modified request message ANM is rejected.

32

33 1.7 Logging

1 In the case where the destination address EA can be addressed,
2 a check is also carried out to determine whether the
3 destination address EA corresponds to one of the logging
4 destination addresses XEA for which a second network element
5 NW2 is to separately record the data quantity. If this is the
6 case, a new first data record DS1 is created for the amount of
7 data in the second network element NW2, that preferably should
8 contain at least the following data record elements:

- 9 - unique identity of the data record;
10 - destination address EA accessed by the communication unit
11 KE;
12 - data quantity;
13 - number of accesses to this destination address EA.

14
15 If the destination address EA corresponds to none of the
16 logging destination addresses XEA, a new second data record DS2
17 for the data quantity is created, that preferably includes the
18 following data record elements:

- 19 - unique identity of the data record;
20 - data quantity.

21 This second data record DS2 or the data record element with
22 details of the data quantity is then always updated if one or
23 more messages, possibly containing useful data ND, that
24 according to the relevant filter instruction FW correspond to
25 none of the logging destination addresses XEA, are exchanged
26 between the communication unit KE and a destination address EA.

27
28 All first or second data records DS1 or DS2 are stored in a
29 logfile PD on a storage element SM.

30
31 From the modified request message ANM, an eighth message N8 is
32 then generated that is forwarded to a downstream second network
33 unit NW2 or to a unit addressed by the destination address EA.

1 This second network unit NE2 is located in the public packet-
2 oriented network PN. The answer to this eighth message N8,
3 realized in Figure 2 as the ninth message N9, is, after receipt
4 by the second network element NW2, allocated to the
5 corresponding data record DS1 or DS2 with which the modified
6 request message ANM has already been logged. Following this,
7 the second network element NW2 sends the ninth message N9 to
8 the communication unit KE by means of a seventh message N7.
9

10 1.8 Evaluation of the logfile

11 At a later timepoint, the second network element NW2 can
12 forward the logfile PD via an eighth connection V8 to an
13 evaluation unit AWE, for example a call-charging point, by
14 means of a logging message PDN. This evaluation unit AWE
15 evaluates one or more first or second data records DS1 or DS2
16 of the logfile PD, for example to generate a bill for the
17 communication unit KE.

18
19 Furthermore, one or more first or second data records DS1 or
20 DS2 for the volume of data can be evaluated by the evaluation
21 unit AWE to enable control information to be generated for the
22 optimization of data traffic within one or more networks, for
23 example for the home network HN.

24
25 The use of filter instructions FW is advantageous in this
26 respect because this contains billing depending upon the
27 transmitted content, e.g. of useful data ND. Thus, accesses to
28 a presence server can be separately recorded in that the
29 address of the presence server is filtered. It is also
30 advantageous in practice if the billing is not dependent on the
31 low-level transport network, such as the GPRS. The generation
32 of data records such as the first data record DS1 for recording
33 the volume of data takes place merely in a network element of

1 the data gateway type e.g. in the second network element NW2 in
2 the exemplary embodiment shown here. A lower-level GPRS
3 transport network will possibly offer the connection between
4 the communication unit KE and the first network element NW1
5 that leads directly to the second network element NW2 free of
6 charge. The billing then also takes place in the case of GPRS
7 merely via the second and/or third network element NW2 or NE3.
8 The GPRS transport network is thus not required to provide a
9 billing function.

10

11 1.9 Expansions and variations

12 A possible expansion of the exemplary embodiment is explained
13 in more detail with the aid of Figure 1 and Figure 2. For this
14 purpose, an additional modified second connection V2M is first
15 inserted between the first network element NW1 and the second
16 network element NW2 in the architecture of Figure 1. This
17 modified second connection V2M enables the second network
18 element NW2 to notify the first network element NW1 if it is to
19 disconnect the first connection V1 between the communication
20 unit KE and the first network element NW1. If, for example, the
21 authentication of the communication unit KE fails, the second
22 network element NW2 can then instruct the first network element
23 NW1 to disconnect the first connection V1 and thus again
24 release the radio resource occupied by this first connection
25 V1. To do this, the second network element NW2, after
26 transmitting the tenth message N10, transmits a twelfth message
27 N12 to the first network element NW1 and thus requests the
28 first network element NW1 to disconnect the first connection
29 V1. The twelfth message N12 contains a unique identification of
30 the connection to be disconnected, for example the first
31 connection V1.

32

1 In accordance with an expansion of the method in accordance
2 with the invention, the first network element NW1 allocates a
3 connection identity VID at the start of the configuration of a
4 new communication connection. The configuration of a
5 communication connection in this case means the establishment
6 of one or more connections between the particular network
7 elements NEE and the communication unit KE, so that this
8 communication unit KE can send one or more request messages AN
9 to a second network unit NW2. Several communication connections
10 can exist at the same time for one communication unit KE. For
11 example for three different user identities NID of a
12 communication unit KE three different communication connections
13 exist at the same time. This connection identity VID uniquely
14 identifies a connection between the first and second network
15 element NW1 or NW2 of this new communication connection. The
16 connection between the communication unit KE and the first
17 network element NW1 is also uniquely identifiable with the aid
18 of the IP (Internet Protocol) address, the communication unit
19 KE and this connection identity VID.

20

21 The first network element NW1 forwards this connection identity
22 VID, together with the IP address IPA of the communication unit
23 KE in an eleventh message N11 to the second network element
24 NW2. The second network element NW2 acknowledges the receipt of
25 the eleventh message N11 by means of a fourteenth message N14.
26 This realization variant is advantageous because this merely
27 requires a further signaling between the first and second
28 network elements NW1 or NW2. The unique identification of this
29 communication connection is thus known to the first and second
30 network elements NW1 and NW2. This is useful in practice
31 because one communication network KE can contain several
32 communication connections to a first network element NW1 under
33 the same IP address IPA. If the second network element NW2

1 gives the IP address IPA and the connection identity VID in the
2 twelfth message N12, the first network element NW1 then clearly
3 detects which communication connection or connection between
4 the communication unit KE and the first network element NW1 is
5 to be disconnected. The first network element NW1 acknowledges
6 receipt of the twelfth message N12 by means of a thirteenth
7 message N13.

8

9 The additional signaling with the eleventh and fourteenth
10 messages N11 and N14 can also be used to send GPRS billing
11 information to the second network element NW2. The second
12 network element NW2 can add the GPRS billing information to one
13 or more data records DS1 or DS2 of the second network element
14 NW2 and forward this to the evaluation unit AWE.

15 The evaluation unit AWE can correlate the data records DS1 or
16 DS2 with the billing information of the GPRS transport network,
17 for example with a billing function, and from this generate
18 billing of the connection charges for the communication unit
19 KE.

20

21 As an alternative to using a connection identity VID, an IPSec
22 (Internet Protocol Security) Tunnel IIP can be used. For
23 example, this can occur by means of the use of IPSec technology
24 as in IETF RFC 2401, "Security Architecture for the Internet
25 Protocol". This IPSec Tunnel IIP is assigned an identity. To
26 disconnect the connection between the communication unit KE and
27 the first network element NW1, the second network element NW2
28 merely transmits this identity of the IPSec Tunnel IIP to the
29 first network element NW1. This identity is unambiguously known
30 in both the first and second network elements NW1 and NW2. The
31 first network element NW1 knows the map of the identity for the
32 IPSec Tunnel IIP for the associated connection between the
33 first network element NW1 and the communication unit KE.

1
2 For this solution, an IPSec Tunnel is provided between the
3 first and second network elements NW1 and NW2 for each
4 communication connection of a communication unit KE. This
5 alternative is useful in practice because no additional
6 signaling is required in order to communicate this identity of
7 the IPSec Tunnel to the second network element NW2. The
8 eleventh and fourteenth messages N11 and N14 are not required
9 in this case.

10
11 After successful disconnection of the first connection V1
12 between the communication unit KE and the first network element
13 NW1, that was initiated by the twelfth message N12 through the
14 second network element NW2, the first network element NW1 sends
15 a confirmation message N13 back to the second network element
16 NW2.

17
18 2. Second exemplary embodiment
19 2.1 Device and construction
20 In a further exemplary embodiment, an alternative to
21 authentication and protection of the integrity of a
22 communication unit KE with the aid of a second network element
23 NW2 is described. A second network element NW2 can be realized
24 in the form of a data gateway. Figure 4 shows a possible device
25 for the implementation of this exemplary embodiment. The
26 communication unit KE is located in a visited network VN. One
27 or more messages can be formed with the aid of the SIP (Session
28 Initiation Protocol) syntax, see IETF RFC 3261, "SIP Initiation
29 Protocol".

30
31 The communication unit KE is connected with a first network
32 element NW1 in the searched-for network VN via a first
33 connection V1. This first connection V1 is established using a

1 procedure called "PDP Context Activation Procedure", as
2 described in 3GPP TS 23.06.0 version 5.3.0. This first
3 connection V1 is thus realized with a first PDP context. During
4 the establishment of this first connection V1, it is specified
5 that this may be used only for the exchange of messages between
6 the communication unit KE and the second network element NW2.
7 All messages sent on this first connection V1 are automatically
8 forwarded from the first network element NW1 via a second
9 connection V2 to a second network element NW2. The second
10 network element NW2 has a fourth connection V4 in a public
11 packed-oriented network PN. In addition, the second network
12 element NW2 has a third connection V3 to a SIP-proxy PCS. This
13 SIP-proxy PCS is in this case always in the same network as the
14 first network element NW1, i.e. in the visited network VN in
15 this exemplary embodiment. Furthermore, with the aid of the
16 procedure called "PDP Context Activation Procedure", a further
17 connection called a fifth connection V5 is established between
18 the communication unit KE and the first network element NW1.
19 This fifth connection V5 is realized by means of a second PDP
20 context. This fifth connection V5 is used mainly for the
21 exchange of SIP messages. Furthermore, the first network
22 element NW1 is connected via a sixth connection V6 to the SIP
23 Proxy PCS, that additionally has a seventh connection V7 to the
24 second SIP Proxy SCS. Via the fifth and sixth connections V5
25 and V6, only messages without useful data ND are exchanged
26 between the communication unit KE and the SIP Proxy PCS. The
27 second SIP Proxy SCS is always located in the home network HN
28 of the communication unit KE and mainly has the function of a
29 SIP registrar, see IETF RFC 3261, "SIP Initiation Protocol".
30 The second SIP Proxy SCS has a tenth connection V10 to the
31 database HSS. In order to also exchange SIP messages with one
32 or more communication units KE in the public packet-oriented

1 network PN, the second SIP Proxy SCS is connected by means of a
2 ninth connection V9 to this public packet-oriented network PN.

3

4 With the aid of Figure 5, the messages for exchanges for
5 authentication and protection of integrity and for the
6 distribution of one or more keys in accordance with this
7 exemplary embodiment are explained in more detail. To use one
8 or more IMS (IP Multimedia Subsystem) services, a communication
9 unit KE first registers with the IMS network. The sequence of
10 registration is described in detail in documents IETF RIF 3261
11 and 3GPP TS 24.229, version 5.2.0. "IP Multimedia Call Control
12 Protocol based on SIP and SDP". Furthermore, examples of the
13 message exchange are given in document 3GPP TS 24.228
14 "Signaling Flows for the IP Multimedia Call Control based on
15 SIP and SDP"

16

17 2.2 Request message

18 For registration, the communication unit KE first sends a
19 request message AN named "Register" via the fifth and sixth
20 connections V5 and V6 to the SIP Proxy PCS. This forwards this
21 request message AN to the second SIP Proxy SCS in the home
22 network HN by means of a second message N2. Both the request
23 message AN and the second message N2 contain the user identity
24 NID. The user identity NID used for authentication is, as
25 described in documents IETF RFC 3310 and IETF RFC 2617,
26 contained in the message AN or N2 in an information line with
27 the name "Authorization".

28

29 2.3 Useful information

30 On the basis of this user identity NID the second SIP Proxy SCS
31 now, with the aid of a third message N3, requests one or more
32 items of useful information NI from the database HSS. For
33 further examination, a distinction is made between two

1 different second keys SP2P and SP2N. The one second key is
2 designated in the following as the second proxy key SP2P. This
3 contains at least one key for authentication and protection of
4 integrity and for encoding the connection between the
5 communication unit KE and the SIP Proxy PCS, and is meant for
6 the SIP Proxy PCS. The other second key is designated in the
7 following as the second network key SP2N. This includes at
8 least one key for protecting the integrity and for encoding the
9 connection between the communication unit KE and the second
10 network element NW2, and is meant for the second network
11 element NW2. In the following, it is assumed that precisely one
12 second network key SP2N and one second proxy key SP2P exist.
13 After receipt of the third message N3, the database HSS answers
14 with a fourth message N4 that contains one or more items of
15 useful information NI. One or more items of useful information
16 NI in this case include the second proxy key SP2P and the
17 challenge HEF that is transmitted in a later step to the
18 communication unit KE for authentication. The second SIP Proxy
19 SCS now sends this useful information NI in a fifth message N5
20 with the name "401 Unauthorized" to the SIP Proxy PCS. This
21 fifth message N5 contains both the second proxy key SP2P and
22 also the challenge HEF, both of which are used for
23 authentication of the communication unit KE between the
24 communication unit KE and the second SIP Proxy SCS. The second
25 proxy key SP2P and the challenge HEF are both, in accordance
26 with documents IETF RFC 3310 and IETF RFC 2617, inserted into
27 the fifth message N5 in an information line named "WWW-
28 Authenticate". The SIP Proxy PCS takes the proxy key SP2P for
29 protecting the integrity and for encoding from the fifth
30 message N5 and forwards this modified message in the form of a
31 sixth message N6 to the communication unit KE. On the basis of
32 the information in the challenge HEF, the communication unit KE
33 now generates a first key, designated in the following as a

1 first proxy key SP1P, that is used to protect the integrity and
2 for encoding. Furthermore, the communication unit KE uses the
3 first proxy key SPIP to generate a response AGH to the
4 challenge HEF.

5

6 2.4 Modified request message

7 Subsequently, the communication unit KE sends a modified
8 request message ANM named "Register" to the SIP Proxy PCS. This
9 modified request message ANM contains the response AGH to the
10 challenge. In accordance with documents IETF RFC 3310 and IETF
11 RFC 2617, this modified request message ANM contains this
12 response AGH in an information line named "Authorization".
13 Furthermore, the integrity of this modified request message ANM
14 is protected with the aid of the generated first proxy key
15 SP1P.

16

17 With the aid of the second proxy key SP2P, received from the
18 second SIP Proxy SCS, the SIP Proxy PCS now checks whether the
19 modified request message ANM was changed by the communication
20 unit KE after its generation. If the check of the integrity
21 shows that the integrity is in order, the SIP Proxy PCS
22 forwards this modified request message ANM to the second SIP
23 Proxy SCS in the form of an eighth message N8.

24

25 The second SIP Proxy SCS uses the response AGH to the challenge
26 HEF to check whether the communication unit KE is authorized to
27 register on the IMS network. If the check shows that the
28 communication unit KE is authorized for this purpose, the
29 second SIP Proxy SCS informs the database HSS, by means of a
30 ninth message N9, that the communication unit KE is now
31 registered.

32

33 2.5 Further useful information

1 The database HSS then sends one or more further items of useful
2 information NIW, by means of a tenth message N10, to the second
3 SIP Proxy SCS. One or more further items of useful information
4 NIW include, for example, the second network key NP2N used to
5 protect the integrity and for encoding for the connection
6 between the communication unit KE and the second network
7 element NW2. Furthermore, one or more filter instructions FW
8 are contained, that are used to filter the message traffic from
9 the second network element NW2. Alternatively, to transmit
10 further useful information NIW by means of a tenth message N10,
11 these further items of useful information NIW can already have
12 been transmitted with one or more items of useful information
13 NI in the fourth message N4. One or more filter instructions FW
14 are generated in accordance with the previous exemplary
15 embodiment.

16

17 In the next step, the second SIP Proxy SCS sends an eleventh
18 message N11 with the name "200 OK" to the SIP Proxy PCS. This
19 eleventh message N11 contains one or more second network keys
20 SP2N for protecting the integrity and for encoding, that are
21 used by the second network element NW2. Furthermore, this
22 eleventh message N11 also contains additional information
23 required by the communication unit KE, in order for it to
24 calculate a first network key SP1N. A first network key SP1N
25 and a second network key SP2N together form a correlated key
26 pair SCP for protecting the connection between the second
27 network element NW2 and the communication unit KE.

28

29 Alternatively, a common key pair SCP can be used instead of
30 different keys for the particular connection between the
31 communication unit KE and the second network element NW2 and
32 between the communication unit KE and the SIP Proxy PCS.

33

1 2.6 User identity

2 Several user identities NID can be allocated to one
3 communication unit KE. In this case in an advantageous
4 expansion, it is useful in practice to additionally allocate
5 one or more user identities, with which the particular key may
6 be used, to one or more keys. The second network element NW2
7 can permit the exchange of messages between the communication
8 unit KE and the second network element NW2 by using a specific
9 user identity, such as the first user identity NID1, or reject
10 it under a different user identity, such as the first user
11 identity NID2. The generation of different user profiles for
12 one communication unit is thus possible.

13

14 The SIP Proxy PCS takes the second network key SP2N and all
15 filter instructions FW from the eleventh message N11. Using the
16 name "200 OK" of this eleventh message N11, the SIP Proxy PCS
17 detects that the authentication was successful.

18

19 The SIP Proxy PCS sends this modified eleventh message N11 as
20 the fourteenth message N14 to the communication unit KE. With
21 the help of the information contained in this fourteenth
22 message N14, the communication unit now calculates a first
23 network key SP1N for protecting the integrity and for encoding.
24 This first network key SP1N is used for message exchange
25 between the communication unit KE and the second network
26 element NW2. Furthermore, the SIP Proxy PCS uses a twelfth
27 message N12 to forward its network key SP2N and all filter
28 instructions FW to the second network element NW2, that
29 confirms receipt by means of a thirteenth message N13.

30

31 2.7 Message exchange

32 In the following, the communication unit KE and the second
33 network element NW2 can exchange messages with each other. This

1 is explained in more detail with the aid of Figure 6. The
2 communication unit KE sends a request message AN to the second
3 network element NW2. This request message AN contains the user
4 identity NID and the required destination address EA from which
5 useful data ND is requested. In the case where the HTTP
6 protocol is used, this request message AN is an HTTP request.
7 This request message AN is protected with the aid of a first
8 network key SP1N to protect the integrity and can be encoded.
9 With one of its network keys SP2N, the second network element
10 NW2 is able to encode the received request message AN and to
11 check whether this request message AN was changed by the
12 communication unit KE after it had been generated. The second
13 network element NW2 then checks whether the transmitted user
14 identity NID can be used together with the used first network
15 key SP1N or the corresponding second network key SP2N, and the
16 communication unit KE is thus authorized to send one or more
17 messages.

18
19 In a case where the communication unit KE is authorized to send
20 one or more messages, the second network element NW2 also
21 checks, with the aid of the filter instructions FW received
22 from the SIP Proxy PCS, whether the communication unit KE can
23 access the destination address EA contained in the request
24 message AN by means of the user identity NID used by it. If
25 this is the case, the second network element forwards this
26 request message AN to the corresponding destination address EA
27 in the form of a sixteenth message N16. Furthermore, the second
28 network element NW2 checks whether it should generate one or
29 more data records for the data volume for access to the
30 required destination address EA. The generation of one or more
31 data records in this case corresponds to the procedure
32 described in the preceding exemplary embodiment.

1 In a case where the communication unit KE is not authorized
2 under the named user identity NID to exchange messages with a
3 second network element NW2 or under the named user identity NID
4 is not permitted in accordance with one or more filter
5 instructions FW to access the required destination address EA,
6 the second network element NW2 sends back an eighteenth message
7 N18 to the communication unit KE. This eighteenth message N18
8 notifies the communication unit KE that it is not authorized,
9 under the named identity NID, to access the named destination
10 address EA.

11

12 Finally, one or more data records can be transmitted via an
13 eighth connection V8 to an evaluation unit AEW for evaluation.
14

15 3. Third exemplary embodiment -

16 association of SIP signaling and messages

17 In accordance with an expansion of the method in accordance
18 with the invention, the following exemplary embodiment is used
19 to describe how one or more messages with useful data ND
20 between a communication unit KE and a second network element
21 NW2 can be associated with a signaling transaction. For this
22 purpose, it is assumed that the communication unit KE is
23 already registered on the IMS network and thus the
24 authorization has been successfully completed and also the
25 corresponding key for protecting the integrity and encoding in
26 the second network element NW2 and in the communication unit KE
27 are present. The message flow for this exemplary embodiment is
28 explained in more detail with the aid of Figure 7. In addition
29 to the network elements known from Figure 4, a new network
30 element named the application server AS is introduced for this
31 exemplary embodiment. In this exemplary embodiment the
32 application server AS is a presence server.

33

1 The purpose of the application server AS is to instruct the
2 communication unit KE regarding the changing of an item of
3 presence information of a further communication unit, possibly
4 communication unit KE2. Where the SIP protocol is used for
5 signaling, the application server AS in this case uses a SIP
6 message with the name "Notify". In this case it is appropriate
7 that the SIP message named "Notify" additionally contains the
8 current presence information PI. If this presence information
9 PI is very large, it is advantageous in practice if it is not
10 transferred via the same connection as the other SIP messages,
11 so that one or more SIP proxies, for example SIP proxy CPS or
12 second SIP proxy SCS are not overloaded. A possible procedure
13 for this is described in document "Draft-IETS-SIP-CONTENT-
14 INDIRECT-MECH-00", "A mechanism for content indirection in SIP
15 messages", see www.ietf.org, with which a communication unit is
16 diverted to a destination address containing one or more items
17 of useful data ND. This useful data ND corresponds in this
18 embodiment to the current presence information PI. A diversion
19 information UNI is contained in the SIP message for this
20 purpose. This includes, for example, a diverted destination
21 address UNI where this presence information PI is to be found.
22 Furthermore, it indicates the protocol, for example HTTP, to be
23 used to request this presence information PI.

24
25 First, the application server AS with the aid of a first
26 message NI sends the diversion information UNI to the second
27 SIP Proxy SCS, that also indicates that presence information PI
28 of a second communication KE2 is available at a diverted
29 destination address UEA. This presence information PI is meant
30 for the communication unit KE. The second SIP Proxy SCS expands
31 this first message NI by adding an acquisition identity EI. The
32 acquisition identity EI clearly identifies a SIP transaction,
33 i.e. in this case the notification of the communication unit KE

1 regarding the presence information PI of the second
2 communication unit KE2. It is possible to signal this
3 acquisition identity EI with the aid of an information line
4 with the name "Media-Authorization" (see IETF RFC 3310) in a
5 message. This acquisition identity EI indicates that those
6 messages are to be separately acquired that are to be exchanged
7 between the communication unit KE and the second network
8 element NW2 on the basis of the diversion information UNI
9 contained in this first message NI.

10

11 In a next step, the second SIP Proxy SCS sends this expanded
12 message in the form of a second message N2 to the SIP Proxy
13 PCS. This second message N2 contains the diversion information
14 UNI and the acquisition identity EI. Furthermore, the second
15 SIP Proxy SCS can also specify the number of permitted accesses
16 and/or the time duration in which the accesses to the diverted
17 destination address UEA are permitted. Furthermore, the second
18 SIP Proxy SCS generates a data record DS that can subsequently
19 be used for controlling and evaluating the message traffic.
20 This data record DS preferably contains the following data
21 record elements:

- 22 - Type of message from the application server AS, for
23 example type "Notify" or "Info" SIP message;
24 - Diverted destination address UEA to which reference was
25 made in the particular message;
26 - Acquisition identity EI;
27 - User identity NID.

28

29 As an alternative, a data record DS can already be generated
30 and the acquisition identity EI created by the application
31 server AS instead of the second SIP Proxy SCS.

32

1 The SIP Proxy PCS forwards the second message N2 in the form of
2 a third message N3 to the communication unit KE. In parallel
3 with this, the SIP Proxy PCS sends a fourth message N4 to the
4 second network element NW2. This fourth message N4 informs the
5 second network element NW2 that it is to separately acquire the
6 message traffic with the communication unit KE, if the
7 acquisition identity EI is contained in the messages of the
8 communication unit KE. The acquisition identity EI and the
9 diverted destination address UEA that can be accessed by means
10 of this acquisition identity EI are contained in the fourth
11 message N4 for this purpose. This is advantageous in practice
12 because the second network element NW2 thus has the capability
13 of using this acquisition identity EI to stop messages to
14 destination addresses other than the diverted destination
15 address UEA. Furthermore, the user identity NID with which the
16 communication unit KE can send messages with this acquisition
17 identity EI is also contained in the fourth message N4.

18

19 Furthermore, this fourth message N4 can contain repetition
20 information that indicates how often the communication unit KE
21 may use the acquisition identity EI. If messages on the
22 connection between the communication unit KE and the second
23 network element NW2 are lost, this repetition information can
24 be used to indicate how often the communication unit KE can
25 repeatedly send this message. A multiple transmission of a
26 specific message with the same acquisition identity EI is thus
27 enabled. However, the possibility of a communication unit KE
28 using the same acquisition identity EI for additional messages
29 is limited. This repetition information can also be already
30 transmitted from the second SIP Proxy SCS to the SIP Proxy PCS
31 in the second message N2.

32

1 The SIP Proxy PCS and the second network element NW2 are always
2 located in the same network, for example in Figure 4 in the
3 visited network VN. Meanwhile, when "roaming" the second SIP
4 Proxy SCS can be in a different network than the communication
5 unit, for example in Figure 4 in the home network HN.
6 Therefore, the SIP Proxy PCS knows which type of connection,
7 for example lossy or lossless, is supported and used by the
8 second network element NW2.

9

10 The second network element NW2 now confirms receipt of the
11 fourth message N4 by means of a fifth message N5. The
12 communication unit KE confirms receipt of the third message N3
13 by using a sixth message N6. After receipt of this sixth
14 message N6, the SIP Proxy PCS forwards this message in the form
15 of a seventh message N7 to the second SIP Proxy SCS, that then
16 forwards this seventh message N7 in the form of an eighth
17 message N8 to the application server AS. In this way, the
18 application server AS knows that the communication unit KE has
19 received diversion information UNI.

20

21 Subsequently, the communication unit KE sends a request message
22 AN to the second network element NW2, in order to request one
23 or more items of useful data ND from the diverted destination
24 address UEA given in the third message N3. If the HTTP protocol
25 is used for the request message AN, this is an HTTP request.
26 This includes both the diverted destination address UEA and the
27 user identity NID. This user identity NID is contained in the
28 information line with the name "Authorization" in this request
29 message AN, as described in IETF RFC 3310 and IETF RFC 2617. In
30 addition, the acquisition identity EI is integrated into this
31 request message AN.

32

1 In a possible expansion of the exemplary embodiment in which
2 the HTTP protocol is used for the request message AN, this
3 acquisition identity EI can be contained in an information
4 line, to be redefined with the name "Access Authorization".
5

6 The second network element NW2 uses the information received
7 from the SIP Proxy PCS to check whether the communication unit
8 KE is authorized under the user identity NID contained in the
9 request message AN to access the given diverted destination
10 address UEA by specifying the acquisition identity EI. If the
11 check shows that access is permitted, the second network
12 element NW2 forwards this access message AN to the diverted
13 destination address UEA. This takes place in the form of a
14 tenth message N10. Furthermore the second network element now
15 separately acquires the message exchange on the basis of this
16 request message AN. For this purpose, the second network
17 element creates a second data record DS2 that advantageously
18 contains the following data record elements:

- 19 - Acquisition identity EI;
20 - Diverted destination address UEA which the communication
21 unit KE accesses;
22 - User identity NID;
23 - Size of all messages;
24 - Number of messages that were exchanged under the
25 acquisition identity EI.

26
27 The answer to the tenth message N10 is sent to the second
28 network element NW2 by means of an eleventh message N11. This
29 eleventh message N11 is acquired in the second data record DS2
30 and then forwarded to the communication unit KE in the form of
31 a twelfth message N12.

1 In the case where the communication unit KE was not authorized
2 to send the request message AN to the second network element
3 NW2, the second network element NW2 sends back a thirteenth
4 message N13 to the communication unit KE. This thirteenth
5 message N13 states that the request message AN was not
6 forwarded. In this case, the tenth, eleventh and twelfth
7 messages N10, N11 and N12 are not sent.

8

9 3.1 Evaluations of data records

10 In a next step, the second network element NW2 can send this
11 second data record DS2 to an evaluation unit AWE, for example a
12 call-charging center, for evaluation and controlling. In
13 addition, the data record DS can also be forwarded to the
14 evaluation unit AWE.

15

16 With the help of both data records DS and DS2, the evaluation
17 unit AWE can now correlate the messages with signaling
18 information, thus for example the SIP transactions, and the
19 messages between the communication unit KE and the second
20 network element NW2. The acquisition identity EI in this case
21 identifies the particular messages that were generated on the
22 basis of a specific SIP transaction. This is advantageous in
23 practice because those messages between the communication unit
24 KE and the second network element NW2, that have been triggered
25 by SIP signaling, can be evaluated differently, e.g. charged,
26 from the other message traffic. For example, messages with
27 useful data ND that contain images or Internet pages can be
28 charged at a higher tariff than those messages that were
29 generated by the SIP signaling. In addition, an evaluation
30 criterion can be derived relative to the data volume of the
31 transmitted messages. For example where a larger quantity of
32 data is transmitted the price for each unit of transmitted data
33 is more favorable. Besides this, an evaluation criterion using

1 accesses to specific destination addresses can be generated.
2 Thus, for example, chargeable call services can be allocated to
3 certain destination addresses, e.g. requesting a telephone
4 number from an Internet-based telephone information service.
5 Accesses to these specific destination addresses are billed at
6 a special rate on the basis of this selection criterion.

7
8 In addition, repeated accesses to a destination address can be
9 evaluated differently. The initial access to a certain
10 destination address may possibly be free of charge, whereas
11 each further access incurs a charge. In practice, it can also
12 be useful to make the analysis of the transmitted messages
13 relative to the transmitted user identity NID. A certain user
14 identity ID can, for example, be allocated to a specific
15 application AP that can be used free of charge.

16
17 In addition to the evaluation of one or more data records for
18 the purpose of billing a communication unit, the evaluation
19 unit AWE can also control and/or optimize the message traffic
20 within one or more networks. For example, destination address
21 of a data server that contains useful data to which frequent
22 accesses are made and which cause a large amount of data to be
23 transferred can thus be filtered out. In a further step, this
24 useful data can possibly be copied to several data servers in
25 different networks, in order to improve the distribution of the
26 transmitted data volume.

27